NIH Standards for Establishing Data Quality and Management Protocols for Trusted Partner Relationships

Data Submission	
Policy	I. Adherence to the NIH Institutional Certification process for submission of data
Technical	I. Data specifications: A. Contracts must stipulate: 1. Unrefined (e.g., prepublication) versions of individual-level data 2. Aggregate summary results, when they are available and clearly part of the analysis result 3. Summary-level information of the main individual phenotype or exposure variables and any covariates 4. Summary-level information of the genomic region(s) analyzed and factors that affect genomic properties, such as the study population, specimen tissue type, tissue origin, and developmental stage B. Data file types and formats must include: 1. Indication of the type and accuracy of instrument data 2. Metadata—sufficient context and description for users to identify and obtain individual-level data of interest 3. Methods—sufficient context and description of process used to create data (e.g., workflow, tools versions)
	II. Data quality requirements: A. Contracts must describe the quality assurance process and critical quality control steps that must be performed prior to making data available for distribution or as a part of long-term data maintenance
	III. Availability and resilience measures: A. Where possible, community standards should be applied to the data submission system that address factors such as: 1. Uptime 2. Time to recover on failure 3. Response time to resolve information technology (IT) problems 4. Percentage successful downloads/requests
Data Storage	
Policy	I. NIH maintains the expectation that all data accepted to the trusted partner data repository are de-identified according HHS Regulations for the Protection of Human Subjects (45 CFR 46.102(f)) and the HIPAA Privacy Rule (45 CFR 164.514(b)). The data will be provided with a random, unique code that is held by the submitting institution.
Technical	I. Capacity for growth—data capacity should accommodate the anticipated needs of the project, particularly with rapid advances in technology leading to increased amounts and complexity of data; it should be evaluated by considering factors such as: A. Percentage of space used/available B. Rate of space utilization (actual vs. predicted) C. Percentage of network bandwidth used D. Rate of bandwidth growth

Data Distribution	
Policy	I. Data will be maintained through controlled access: A. Permission to access data will be requested through NIH Data Access Committees, per NIH-prescribed processes for the institutional certification of data sharing requests B. Standard telemetry will be used to communicate with NIH systems for authenticating Approved Users through the dbGaP data request process
Technical	I. Data will be encrypted during transmission II. Data will remain encrypted when stored on trusted partner computers having direct access to the internet or be placed in an isolated network (enclave) with access to specific data available only to those authorized by the NIH and authenticated for data access III. The trusted partner needs to accommodate the investigators' needs to comply with reporting (e.g., renewal requests and close out reports)
Data Security	
Policy	I. At a minimum, policies, procedures, controls, and standards comparable to the HHS Information Security Program to ensure the integrity, confidentiality, and availability of Federal information systems must be adopted and implemented (http://www.hhs.gov/ocio/index.html)
Technical	I. Security policies and procedures, which should be continually updated, must be in place that incorporate the following items at a minimum: A. Training of personnel B. Physical security of the network and system C. Physical security of the server facilities D. User authentication and activity logging 1. Systems to track system usage 2. Monthly reports of data input/output information E. System intrusion prevention and detection II. Documentation should be provided and reviewed at a minimum of every three years for a(n): A. Technical IT security plan B. IT risk assessment C. Federal Information Processing Standards (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems Assessment D. Security control testing and evaluation results III. Completion of an independent Federal Information Security Management (FISMA) Act security audit and implementation of security controls or security mitigations before the status as an NIH trusted partner is authorized by the NIH IC IV. Documentation that security plans have been reviewed and approved by an appropriate organizational authority at the trusted partner location (e.g., IT Director, Dean of Research, or Chief Information Officer)
Stewardship	
Policy	I. All data are the property of the NIH and cannot be sold, redistributed, or otherwise transferred without the authorization of the NIH[i] II. All trusted partners must comply with Section 508 of the Rehabilitation Act of 1973 regarding electronic and information technology accessibility
Technical	I. Contracts should document: A. Responsibilities for each party (e.g., trusted partner, NIH staff)

	B. Procedures for reporting and handling data management incidents C. Project close-out plans for the end of the contract period or if the contract is prematurely terminated including: 1. Description of the policy and storage facility if data are transferred to another database with NIH authorization 2. Method of data transfer and specified maximum allowable time for transfer (e.g., three months) 3. Description of data destruction procedures from institutional systems and mobile devices, if data are not retained or transferred

[i] *Solicitation Provisions and Contract Clauses, Federal Acquisition Regulation 52.227-17 Rights in Data-Special Works (d) Release and use restrictions*. Except as otherwise specifically provided for in this contract, the Contractor shall not use, release, reproduce, distribute, or publish any data first produced in the performance of this contract, nor authorize others to do so, without written permission of the Contracting Officer. (e) *Indemnity*. The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability, including costs and expenses, incurred as the result of the violation of trade secrets, copyrights, or right of privacy or publicity, arising out of the creation, delivery, publication, or use of any data furnished under this contract; or any libelous or other unlawful matter contained in such data. The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to material furnished to the Contractor by the Government and incorporated in data to which this clause applies.